Fundamenta Informaticae XXI (2001) 1001–1021
DOI 10.3233/FI-2012-0000
IOS Press

Vector Ambiguity and Freeness Problems in SL$(2, \mathbb{Z})$

Sang-Ki Ko
Artificial Intelligence Research Center
Korea Electronics Technology Institute
22 Daewangpangyo-ro, Gyeonggi-do, 13488, Republic of Korea
sangkiko@keti.re.kr

Igor Potapov
Department of Computer Science
University of Liverpool
Ashton Street, Liverpool, L69 3BX, United Kingdom
sangkiko@liverpool.ac.uk

Abstract. We study the vector ambiguity problem and the vector freeness problem in SL$(2, \mathbb{Z})$. Given a finitely generated $n \times n$ matrix semigroup S and an n-dimensional vector $\mathbf{x}$, the vector ambiguity problem is to decide whether for every target vector $\mathbf{y} = M\mathbf{x}$, where $M \in S$, M is unique. We also consider the vector freeness problem which is to show that every matrix M which is transforming $\mathbf{x}$ to $M\mathbf{x}$ has a unique factorization with respect to the generator of S. We show that both problems are NP-complete in SL$(2, \mathbb{Z})$, which is the set of 2×2 integer matrices with determinant 1. Moreover, we generalize the vector ambiguity problem and extend to the finite and k-vector ambiguity problems where we consider the degree of vector ambiguity of matrix semigroups.

Keywords: matrix semigroup, special linear group, vector ambiguity, vector freeness, decidability, NP-completeness

1. Introduction

Many computational problems for matrix semigroups and groups are proven to be undecidable starting from dimension three or four. On the other hand, a lot of questions for matrix semigroups in dimension two are open including the membership, vector reachability, scalar reachability problems and various problems on freeness. In this paper, we show decidability and reveal complexity of several questions for matrix semigroups in SL$(2, \mathbb{Z})$, which is called the special linear group. The special linear group SL$(2, \mathbb{Z})$ has been extensively exploited in hyperbolic geometry [11, 14, 31], dynamical systems [24], Lorenz/modular knots [21], braid groups [25], high energy physics [29], M/string theories [15], music theory [23], and so on.

Let $S = \langle G \rangle$ be a matrix semigroup finitely generated by a generating set G. The *membership problem* is to decide whether or not a given matrix M belongs to the matrix semigroup S. By restricting

M to be the identity or zero matrix, we call the problems the *identity problem* or *mortality problem*, respectively.

The *vector reachability problem*, which is a parameterized version of the membership problem, can be defined as follows: Given a finitely generated matrix semigroup S of $n \times n$ matrices and two vectors $\mathbf{x}, \mathbf{y}$ in dimension n, the vector reachability problem decides whether or not there exists a matrix M in S such that $M\mathbf{x} = \mathbf{y}$.

Due to its effective symbolic representation of matrices in SL$(2,\mathbb{Z})$, many decidability and complexity results have been established. For instance, it has been shown that the mortality, identity and vector reachability problems were at least NP-hard for SL$(2,\mathbb{Z})$ in [2, 6], but for the finitely generated subgroups of the modular group, the membership was shown to be decidable in polynomial time by Gurevich and Schupp [16]. Choffrut and Karhumäki proved that the membership problem is decidable in SL$(2,\mathbb{Z})$, and the identity problem is decidable in $\mathbb{Z}^{2\times 2}$ [13]. Moreover, Bell et al. [3] proved that the identity problem in SL$(2,\mathbb{Z})$ is NP-complete by developing a new effective technique to operate with compressed word representations of matrices. The decidability of the membership problem for matrix semigroups in dimension two over integers, rationals or complex numbers is an open question and the only known decidability result that is beyond SL$(2,\mathbb{Z})$ is the first algorithm for the membership problem for non-singular 2×2 integer matrices shown in [27].

Another fundamental problem for matrix semigroups is the *freeness problem*, where we want to know whether every matrix in the matrix semigroup has a unique factorization over G. Mandel and Simon [22] showed that the freeness problem is decidable in polynomial time for matrix semigroups with a single generator for any dimension over rational numbers. [1] Klarner et al. [17] proved that the freeness problem in dimension three over natural numbers is undecidable. Along with the membership problem, the freeness problem in dimension two is also an open problem for a long time [8, 9] except certain special cases. For example Charlier and Honkala [12] showed that the freeness problem is decidable for upper-triangular matrices in dimension two over rationals when the products are restricted to certain bounded languages. Bell and Potapov [5] showed that the freeness problem is undecidable in dimension two for matrices over quaternions. Recently, the freeness problem in SL$(2,\mathbb{Z})$ is proven to be NP-complete where NP-hardness is shown in [18] by the reduction from the *equal subset sum problem* (ESSP) [30] and the NP algorithm is given in [3].

In case of vector (scalar) reachability, the question about uniqueness of transformations with respect to the given initial vector can be related to two different interpretations: the vector (scalar) ambiguity and vector (scalar) freeness. Let S be a matrix semigroup of $n \times n$ matrices and $\mathbf{x}$ be an n-dimensional vector. Bell and Potapov [4] showed that the problem of deciding whether S and $\mathbf{x}$ generate a non-repetitive set of vectors—the *vector ambiguity problem*—is undecidable in dimension four over integers and in dimension three over rationals. They used the fact that the problem of determining if a two-counter machine has a periodic configuration is undecidable. Recently, the *scalar ambiguity and freeness problems* have been introduced [1]. In the scalar ambiguity and freeness problems, given a matrix semigroup S and two vectors $\mathbf{x}, \mathbf{y}$, we examine the set $\{\mathbf{x}^T M \mathbf{y} \mid M \in S\}$ of scalars and check whether there exists a unique matrix or a unique factorizations of matrices for each scalar. In 2016, Bell et al. [1] showed that both problems are undecidable over bounded languages.

In this paper, we study the *vector ambiguity problem* for matrix semigroups in SL$(2,\mathbb{Z})$ and show

[1] The freeness problem for matrix semigroups with a single generator is the complementary problem of the *matrix torsion problem* which asks whether there exist two integers $p, q \geq 1$ such that $M^p = M^{q+p}$.

that the problem is decidable. Moreover, we prove that the vector ambiguity problem in $\mathrm{SL}(2,\mathbb{Z})$ is NP-complete. We prove the NP-hardness of the vector ambiguity problem in $\mathrm{SL}(2,\mathbb{Z})$ by the reduction from the *subset sum problem* and the membership in NP by the recent result that the identity problem in $\mathrm{SL}(2,\mathbb{Z})$ is in NP [3]. We also examine the *vector freeness problem* in which we analyze the unique factorization of matrices leading to the same vector and show that the problem is also NP-complete in $\mathrm{SL}(2,\mathbb{Z})$. Moreover, we generalize the vector ambiguity problem and extend to the finite and k-vector ambiguity problems where we consider the degree of vector ambiguity of matrix semigroups. In the table below, we are summarizing the results of this paper and position them in the context of currently known results in this area. Bold entries represent new results and dash line '—' means that ambiguity problems for matrix semigroups cannot be defined.

Problem	Domain	Matrix Reachability	Vector Reachability
Non-freeness	$\mathrm{SL}(2,\mathbb{Z})$	NP-complete [18]	**NP-complete**
	$\mathbb{N}^{3\times 3}$	Undecidable [17]	**Undecidable**
k-non-freeness	$\mathrm{SL}(2,\mathbb{Z})$	EXPSPACE [18]	
	$\mathbb{N}^{3\times 3}$	Undecidable [17]	**Undecidable**
Finite non-freeness	$\mathrm{SL}(2,\mathbb{Z})$	EXPSPACE [18]	
	$\mathbb{N}^{3\times 3}$		**Undecidable**
Ambiguity	$\mathrm{SL}(2,\mathbb{Z})$	—	**NP-complete**
	$\mathbb{Z}^{4\times 4}$	—	Undecidable [4]
k-ambiguity	$\mathrm{SL}(2,\mathbb{Z})$	—	EXPSPACE
	$\mathbb{Z}^{4\times 4}$	—	Undecidable [4]
Finite ambiguity	$\mathrm{SL}(2,\mathbb{Z})$	—	EXPSPACE
	$\mathbb{Z}^{4\times 4}$	—	Undecidable [4]

2. Preliminaries

In this section we formulate several problems, provide important definitions and notation as well as several technical lemmas used throughout the paper.

Basic definitions. A *semigroup* is a set equipped with an associative binary operation. Let S be a semigroup and X be a subset of S. Then, X is a *code* if and only if every element of S has a unique factorization over X. A semigroup S is *free* if there exists a subset $X \subseteq S$ which is a code and $S = X^+$.

Given an alphabet Σ, a word w is an element of Σ^*. For a letter $a \in \Sigma$, we denote by $\overline{a}$ the inverse letter of a such that $a\overline{a} = \varepsilon$ where ε is the empty word.

A *nondeterministic finite automaton* (NFA) is a tuple $A = (\Sigma, Q, \delta, q_0, F)$ where Σ is the input alphabet, Q is the finite set of states, $\delta\colon Q \times \Sigma \to 2^Q$ is the multivalued transition function, $q_0 \in Q$ is the initial state and $F \subseteq Q$ is the set of final states. In the usual way δ is extended as a function $Q \times \Sigma^* \to 2^Q$ and the language accepted by A is $L(A) = \{w \in \Sigma^* \mid \delta(q_0, w) \cap F \neq \emptyset\}$. The automaton

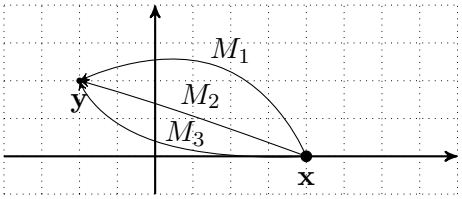

Figure 1. Geometric interpretation of the vector ambiguity problem. If $M_1, M_2, M_3 \in S$, then the matrix semigroup S is ambiguous with respect to the vector $\mathbf{x}$ as there are already three matrices transforming $\mathbf{x}$ into $\mathbf{y}$.

A is a deterministic finite automaton (DFA) if δ is a single valued function $Q \times \Sigma \to Q$. It is well known that the deterministic and nondeterministic finite automata recognize the class of *regular languages* [28].

A *context-free grammar* (CFG) G is a four-tuple $G = (V, \Sigma, R, S)$, where V is a set of variables, Σ is a set of terminals, $R \subseteq V \times (V \cup \Sigma)^*$ is a finite set of productions and $S \in V$ is the start variable. Let $\alpha A \beta$ be a word over $V \cup \Sigma$, where $A \in V$ and $A \to \gamma \in R$. Then, we say that A can be rewritten as γ and the corresponding derivation step is denoted $\alpha A \beta \Rightarrow \alpha \gamma \beta$. The reflexive, transitive closure of $\Rightarrow$ is denoted by $\overset{*}{\Rightarrow}$ and the context-free language generated by G is $L(G) = \{w \in \Sigma^* \mid S \overset{*}{\Rightarrow} w\}$.

Vector ambiguity problem and freeness problems. Let S be an $n \times n$ matrix semigroup finitely generated by a set $G = \{M_1, M_2, \ldots, M_k\}$ of matrices (a generator) and $\mathbf{x}$ be an n-dimensional vector. Then, we assume that $M \cdot \mathbf{x} = \mathbf{y}$ for a matrix M in S. We can say that a vector $\mathbf{y}$ is reachable from $\mathbf{x}$ by S. If there is a unique matrix M in S that transforms $\mathbf{x}$ into $\mathbf{y}$, we say that $\mathbf{y}$ is *unambiguous* with respect to S and $\mathbf{x}$. Note that $\mathbf{y}$ is *ambiguous* with respect to S and $\mathbf{x}$ otherwise. Denote the set of reachable vectors from $\mathbf{x}$ by multiplying the elements of the matrix semigroup S on the left-hand side by V. Namely, $V = \{\mathbf{y} \mid \mathbf{y} = M\mathbf{x},\ M \in S\}$. If every vector in V is unambiguous with respect to S and $\mathbf{x}$, then we say that the matrix semigroup S is unambiguous with respect to $\mathbf{x}$. In other words, if there is a unique matrix $M\mathbf{x} = \mathbf{y}$ for every target vector $\mathbf{y}$, then we say that the matrix semigroup S is *unambiguous* with respect to $\mathbf{x}$.

Similarly, we say that the matrix semigroup S is *free* with respect to $\mathbf{x}$ if every matrix M which transforms $\mathbf{x}$ into $M\mathbf{x}$ has a unique decomposition with respect to the generator G. Otherwise, S is said to be *non-free* with respect to $\mathbf{x}$. The problem of deciding whether or not a given matrix semigroup S is free (respectively, non-free) with respect to a given initial vector $\mathbf{x}$ is called the *vector freeness (respectively, non-freeness) problem*.

Here we consider the following problems for matrix semigroups in SL$(2, \mathbb{Z})$:

- The vector ambiguity problem: given a matrix semigroup S of $n \times n$ matrices and an n-dimensional vector $\mathbf{x}$, is S ambiguous with respect to $\mathbf{x}$?
- The vector non-freeness problem: given a semigroup S of $n \times n$ matrices and an n-dimensional vector $\mathbf{x}$, is S non-free with respect to $\mathbf{x}$?

Before tackling the problems, we establish relationships between the proposed problems and matrix semigroup freeness problem.

Lemma 2.1. Given a semigroup S of $n \times n$ matrices and an n-dimensional vector $\mathbf{x}$, the following statements hold:

1. if S is free with respect to $\mathbf{x}$, then S is unambiguous with respect to $\mathbf{x}$,
2. if S is free with respect to $\mathbf{x}$, then S is free, and
3. if S is free and unambiguous with respect to $\mathbf{x}$, then S is free w.r.t. $\mathbf{x}$.

Proof:
To prove the first statement, we assume that S is ambiguous with respect to $\mathbf{x}$. This implies that there are two matrices M and M' in S that transform $\mathbf{x}$ into the same vector, say $\mathbf{y}$. Since M and M' are different matrices, they cannot have the same decomposition of matrices. This means that we have two different factorizations of matrices in S transforming $\mathbf{x}$ into $\mathbf{y}$. Therefore, S is not free with respect to $\mathbf{x}$. We can say that if S is free with respect to $\mathbf{x}$, S is unambiguous with respect to $\mathbf{x}$ by the contrapositive.

Now we prove the second statement. Assume that S is not free. Then, there are two factorizations of matrices generating the same matrix M in S. Since $M\mathbf{x} = \mathbf{y}$, we have two factorizations of matrices that transform $\mathbf{x}$ into $\mathbf{y}$. Therefore, we prove that if S is free with respect to $\mathbf{x}$, then S is free.

We prove the contraposition of the last statement: if S is not free with respect to $\mathbf{x}$, then (i) S is not free or (ii) ambiguous with respect to $\mathbf{x}$.

Assume that S is not free with respect to $\mathbf{x}$. This means that we have two different factorizations of matrices transforming $\mathbf{x}$ into the same vector $\mathbf{y}$. There are two possible cases to consider. The first case is that the two factorizations form the same matrix M. In this case, S has two factorizations for the matrix M. Therefore, S is not free. The second case is that we have two factorizations for two different matrices M and M' such that $M\mathbf{x} = M'\mathbf{x}$. It is easy to see that S is unambiguous with respect to $\mathbf{x}$. □

Group alphabet encodings. Let us introduce several technical lemmas that will be used in encodings for NP-hardness results. Our original encodings require the use of group alphabet and the following lemmas for showing the transformation from an arbitrary group alphabet into a binary group alphabet and later into matrix form that is computable in polynomial time.

It is well-known that $\{cd^ic^{-1} \mid i \geq 1\}$ freely generates a free subgroup of the free group $\langle c, d\rangle$ [7] and that the matrices $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ freely generates a free subgroup of SL$(2,\mathbb{Z})$ [20].

Let $\Sigma = \{z_1, z_2, \ldots, z_l\}$ be a group alphabet and $\Sigma_2 = \{c, d, \overline{c}, \overline{d}\}$ be a binary group alphabet. Define the mapping $\alpha : \Sigma \to \Sigma_2^*$ by: $\alpha(z_i) = c^i d\overline{c}^i, \alpha(\overline{z_i}) = c^i\overline{d}\overline{c}^i$, where $1 \leq i \leq l$. It is easy to see that α is a monomorphism. Note that α can be extended to domain Σ^* in the usual way. We also define a monomorphism $f : \Sigma_2^* \to \mathbb{Z}^{2\times 2}$ as follows:

$$f(c) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad f(\overline{c}) = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}, \quad f(d) = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \quad f(\overline{d}) = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}.$$

The composition of two monomorphisms α and f gives us the following lemma that ensures that encoding the *subset sum problem* (SSP) and the *equal subset sum problem* (ESSP) [30] instances into matrix semigroups can be done in polynomial time.

Lemma 2.2. (Bell and Potapov [4])
Let $z_j \in \Sigma$. For any $i \in \mathbb{N}$, $f(\alpha(z_j^i)) = f((c^j d\overline{c}^j)^i) = \begin{pmatrix} 1+4ij & -8ij^2 \\ 2i & 1-4ij \end{pmatrix}$.

Lemma 2.3. Let w and w' be any two distinct words in Σ^*. Then, for any non-zero integer t: $f(\alpha(w)) \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^t \neq f(\alpha(w'))$.

Symbolic representation of matrices from SL$(2,\mathbb{Z})$. It is known that $\mathrm{SL}(2,\mathbb{Z})$ is generated by two matrices $\mathbf{S} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\mathbf{R} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, which have respective orders 4 and 6. This implies that every matrix in $\mathrm{SL}(2,\mathbb{Z})$ is a product of $\mathbf{S}$ and $\mathbf{R}$. Since $\mathbf{S}^2 = \mathbf{R}^3 = -\mathbf{I}$, every matrix in $\mathrm{SL}(2,\mathbb{Z})$ can be uniquely brought to the following form:

$$(-\mathbf{I})^{i_0}\mathbf{R}^{i_1}\mathbf{S}\mathbf{R}^{i_2}\mathbf{S}\cdots\mathbf{S}\mathbf{R}^{i_{n-1}}\mathbf{S}\mathbf{R}^{i_n}, \tag{1}$$

where $i_0 \in \{0,1\}$, $i_1, i_n \in \{0,1,2\}$, and $i_j \neq 0 \mod 3$ for $1 < j < n$.

Let $\Sigma = \{s,r\}$ be a binary alphabet. We define a mapping $\varphi : \Sigma \to \mathrm{SL}(2,\mathbb{Z})$ as follows: $\varphi(s) = \mathbf{S}$ and $\varphi(r) = \mathbf{R}$. Naturally, we can extend the mapping φ to the morphism $\varphi : \Sigma^* \to \mathrm{SL}(2,\mathbb{Z})$. Let $M \in \mathrm{SL}(2,\mathbb{Z})$ be a matrix of the form given in Equation (1). Then, we say that the following word is the *canonical word* for M:

$$(ss)^{i_0}r^{i_1}sr^{i_2}s\cdots sr^{i_{n-1}}sr^{i_n}.$$

It is easy to see that every matrix in $\mathrm{SL}(2,\mathbb{Z})$ has a unique canonical word. We also call a word $w \in \Sigma^*$ *reduced* if there is no occurrence of substrings ss or rrr in w. Then, we have the following fact. For every matrix $M \in \mathrm{SL}(2,\mathbb{Z})$, there exists a unique reduced word $w \in \Sigma^*$ such that either $M = \varphi(w)$ or $M = -\varphi(w)$ [20].

We use the following definition throughout the paper for recognizing a matrix semigroup in $\mathrm{SL}(2,\mathbb{Z})$ as a regular language over Σ.

A signed automaton $\mathcal{A} = (\langle Q^+, Q^-\rangle, \Sigma, I, \Delta, \langle F^+, F^-\rangle)$ [26] is a nondeterministic finite-state automaton (NFA) whose final states are divided into two (not necessarily disjoint) subsets F^+ and F^-. A signed automaton $\mathcal{A}$ accepts a *signed language* $L(\mathcal{A}) = \langle L(\mathcal{A})^+, L(\mathcal{A})^-\rangle$ where $L(\mathcal{A})^+$ and $L(\mathcal{A})^-$ consist of words $w \in \Sigma^*$ for which there is an accepting run of $\mathcal{A}$ ending in a state of F^+ and F^-, respectively.

Given a matrix semigroup S with a generating set $G = \{M_1, M_2, \ldots, M_n\}$ in $\mathrm{SL}(2,\mathbb{Z})$, we can construct a signed automaton $\mathcal{A}_S$ which accepts $L(\mathcal{A}_S) = \langle L(\mathcal{A}_S)^+, L(\mathcal{A}_S)^-\rangle$ such that for every matrix M in S, there exists a reduced word $w \in L(\mathcal{A}_S)^+$ or $w \in L(\mathcal{A}_S)^-$, respectively, if $M = \varphi(w)$ or $M = -\varphi(w)$, respectively.

Now we explain the construction of $\mathcal{A}_S$ as follows. Let M be a matrix in the generating set G and can be brought to the form of Equation (1). Then, the word w for M is $(ss)^{i_0}r^{i_1}sr^{i_2}s\cdots sr^{i_{n-1}}sr^{i_n}$. In this way, we obtain words for matrices in $G = \{M_1, \ldots, M_n\}$ and say w_i is a word for M_i. We first a standard NFA $\mathcal{A}' = (Q, \Sigma, \delta, I, F)$ which accepts $\{w_1, w_2, \ldots, w_n\}^*$. Obviously, the size of NFA is exponential in the size of the generating set as each word encoding for matrix is of exponential length. Now we define the signed automaton $\mathcal{A}_S = (\langle Q^+, Q^-\rangle, \Sigma, I_S, \Delta, \langle F^+, F^-\rangle)$ as follows:

- $\langle Q^+, Q^-\rangle = Q \times \{+,-\}$,
- $\Sigma = \{s,r\}$ is an input alphabet,
- $I_S = I \times \{+\}$,

- $\langle F^+, F^- \rangle = F \times \{+,-\}$,

and the transition function Δ is defined based on the transition function δ of $\mathcal{A}'$ as follows. For each transition $p \in \delta(q,\sigma)$, there exist two copies of the transition $(p,+) \in \Delta((q,+),\sigma)$ and $(p,-) \in \Delta((q,-),\sigma)$. Lastly, we add ε-transitions connecting states which are reachable by reading ss or rrr while remembering the number of times we have skipped such occurrences. Recall that ss and rrr correspond to the minus identity matrix $-\mathbf{I}$. Formally, for each pair $((q,s_1),(p,s_2))$ of states, where $q,p \in Q$ and $s_1,s_2 \in \{+,-\}$, such that $(p,s_2) \in \Delta((q,s_1),ss)$ or $(p,s_2) \in \Delta((q,s_1),rrr)$, we add $(p,\overline{s_2}) \in \Delta((q,s_1),\varepsilon)$. Note that $\overline{s_2}$ means the opposite sign of s_2. We can add transitions until there is no state pair which is reachable by the word rr and sss finitely many times.

Next we consider a language which contains all (s,r)-representations of a particular matrix in SL$(2,\mathbb{Z})$.

Lemma 2.4. Let M be a matrix in SL$(2,\mathbb{Z})$. Then, there exists a context-free language over $\Sigma = \{s,r\}$ which contains all unreduced representations $w \in \Sigma^*$ such that $\varphi(w) = M$.

Proof:
Recall that for every matrix $M \in \mathrm{SL}(2,\mathbb{Z})$, there exists a unique reduced word $w \in \Sigma^*$ such that either $M = \varphi(w)$ or $M = -\varphi(w)$ [20]. The word w can be written as $w_1 w_2 \dots w_n$, where $w_i \in \Sigma$ for $1 \le i \le n$.

Let $G_M = (V,\Sigma,P,V_S)$ be a context-free grammar, where $V = \{V_S, A^+, A^-\}$ is a finite set of nonterminals, Σ is an alphabet, P is a finite set of production rules, and V_S is the start nonterminal. We define P to contain the following production rules:

- $V_S \to A_1 w_1 A_2 w_2 A_3 \dots A_n w_n A_{n+1}$,
- $A^+ \to \varepsilon \mid sA^-s \mid rA^+rA^+r \mid rA^-rA^-r \mid A^-A^- \mid A^+A^+$. and
- $A^- \to sA^+s \mid rA^+rA^-r \mid rA^-rA^+r \mid A^-A^+ \mid A^-A^+$,

where $A_i \in \{A^+, A^-\}$ for $1 \le i \le n+1$.

Note that if $M = \varphi(w)$, then there exists an even number of A^-'s from all A_i for $1 \le i \le n+1$ and otherwise, there exists an odd number of A^-'s. Then, it is easy to see that the context-free grammar G_M generates all unreduced words encoding the matrix M by the morphism φ. □

3. Vector Ambiguity and Freeness Problems in SL$(2,\mathbb{Z})$

In this section, we prove that the vector ambiguity and freeness problems are NP-complete. Note that the vector ambiguity problem is undecidable over $\mathbb{Z}^{4\times4}$ and over $\mathbb{Q}^{3\times3}$ [4]. We later show that the vector freeness problem is undecidable over $\mathbb{N}^{3\times3}$.

It was shown in [26] that if there is a matrix M from SL$(2,\mathbb{Z})$ satisfying $M\mathbf{x} = \mathbf{y}$, where $\mathbf{x} = [x_1,x_2]^T$ and $\mathbf{y} = [y_1,y_2]^T$ are vectors from $\mathbb{Z}\times\mathbb{Z}$, then this equation either does not have a solution or all its solutions are given by the following formula

$$M = B\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}^t C = B\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^{tk} C, \tag{2}$$

where $t \in \mathbb{Z}$ and B, C are matrices from SL$(2,\mathbb{Z})$. Let us denote the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ by T from now on Moreover, if $M = BT^{kt}C$ and $M\mathbf{x} = \mathbf{y}$, then $\mathbf{y} = C\mathbf{x} = [d, 0]^T$ and $\mathbf{v} = T^{kt}\mathbf{y} = [d, 0]^T$, where $|d| = \gcd(x_1, x_2) = \gcd(y_1, y_2)$.

First, we state the following property of matrices in SL$(2,\mathbb{Z})$ and later exploit the property to establish the main results of the paper.

Lemma 3.1. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ be two matrices from SL$(2,\mathbb{Z})$. If $a = a'$ and $c = c'$, then $B = A \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^t$ for $t \in \mathbb{Z}$.

Proof:
Since $A, B \in SL(2,\mathbb{Z})$, $\det(A) = ad - bc = 1$ and $\det(B) = ad' - b'c = 1$. Thus,

$$a(d - d') = c(b - b'). \tag{3}$$

If $a = 0$ and $c \neq 0$, then $b - b' = 0$. Now we have $A = \begin{pmatrix} 0 & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} 0 & b \\ c & d' \end{pmatrix}$. Since $\det(A) = \det(B) = 1$, $bc = -1$, we have

$$A = \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & d \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & d' \end{pmatrix}.$$

Then,

$$A \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^t = \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^t = \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & d \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & d \mp t \end{pmatrix}.$$

Since we can always pick t such that $d \mp t = d'$, the lemma holds for the case when $a = 0$ and $c \neq 0$. The case when $a \neq 0$ and $c = 0$ is analogous to the previous case.

Now we consider the case when $a \neq 0$ and $c \neq 0$. Starting from Equation (3), we have $\frac{a}{c} = \frac{b'-b}{d'-d}$. This implies $b' = b + at$ and $d' = d + ct$ for some $t \in \mathbb{Z}$. Since

$$A \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^t = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^t = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & at + b \\ c & ct + d \end{pmatrix},$$

we prove that the lemma holds. □

Lemma 3.2. Let $\mathbf{x} = [x_1, x_2]^T$ be a vector from $\mathbb{Z}^2$ and C be a matrix from SL$(2,\mathbb{Z})$ such that $C\mathbf{x} = [d, 0]^T$, where $|d| = \gcd(x_1, x_2)$. Then, a matrix semigroup S of 2×2 integral matrices from SL$(2,\mathbb{Z})$ is unambiguous with respect to $\mathbf{x}$ if and only if for any matrix B in SL$(2,\mathbb{Z})$, there is at most one matrix M in S which is of the form of $M = BT^tC$, where $t \in \mathbb{Z}$.

Proof:
First we prove that if S is unambiguous with respect to $\mathbf{x}$, then there is at most one matrix $M \in S$ of the form $M = BT^tC$ for any $B \in S$, where $t \in \mathbb{Z}$.

Assume that S is unambiguous with respect to $\mathbf{x}$ and we have two different matrices $M = BT^tC$ and $M' = BT^{t'}C$, where $t \neq t'$. Let us denote the vector $[d, 0]^T$ by $\mathbf{d}$ for notational convenience. Since $C\mathbf{x} = \mathbf{d}$, $BT^t\mathbf{d}$ should not be equal to $BT^{t'}\mathbf{d}$ by the assumption. However, $BT^t\mathbf{d} = BT^{t'}\mathbf{d}$ always holds because $T\mathbf{d} = \mathbf{d}$. Therefore, this contradicts our assumption.

Let us consider the opposite direction and prove that if there is a unique matrix $M \in S$ of form BT^tC, then S is unambiguous with respect to $\mathbf{x}$. Assume, to the contrary, that S is ambiguous with respect to $\mathbf{x}$. This implies that there are two matrices M and M' in S such that $M\mathbf{x} = M'\mathbf{x}$. From Equation (2), we see that both M and M' can be represented in the form of BT^tC for some integer t. Since $M \neq M'$, $M = BT^tC$ and $M' = BT^{t'}C$ such that $t \neq t'$. As this contradicts our assumption, we arrive at a contradiction. □

Now we are ready to show that the vector ambiguity problem in SL$(2,\mathbb{Z})$ is NP-complete.

Theorem 3.3. The vector ambiguity problem for finitely generated matrix semigroups in SL$(2,\mathbb{Z})$ is in NP.

Proof:
Suppose that we are given n matrices $M_1, M_2, \ldots, M_n \in \mathrm{SL}(2,\mathbb{Z})$ as generators of the semigroup S. Namely, $S = \langle M_1, M_2, \ldots, M_n \rangle$. Let $w_1, w_2, \ldots, w_n \in \Sigma^*$ be words encoding the generators, such that $\varphi(w_i) = M_i$ for $1 \leq i \leq n$. Then, we can define a regular language L corresponding to S over $\Sigma = \{s, r\}$ as $L = \{w_1, w_2, \ldots, w_n\}^+$.

Recall that every matrix M that transforms a vector $\mathbf{x}$ into a vector $\mathbf{y}$ can be represented in the form of $M = BT^tC$ where $t \in \mathbb{Z}$ and B, C are matrices from SL$(2,\mathbb{Z})$. Moreover, we can compute two matrices B and C in polynomial time [26]. From Lemma 3.2, we can check whether or not S is ambiguous with respect to $\mathbf{x}$ by checking the existence of two different matrices in S which can be represented as BT^tC with different exponents for t.

We first compute a unique matrix C that transforms a given vector $\mathbf{x} = [x_1, x_2]^T$ into $[\gcd(x_1, x_2), 0]^T$. Then, take a inverse matrix C^{-1} of C and encode the matrix with a word w_C, namely, $\varphi(w_C) = C^{-1}$. Now we let $L' = L \cdot \{w_C\}$.

Then, $\varphi(L') = \{MC^{-1} \mid M \in S\}$. Moreover, we can obtain the following statement for $\varphi(L')$: $\varphi(L')$ has two matrices M and M' such that $M' = MT^t$ for some non-zero integer t if and only if $\varphi(L)$ has two matrices of form BT^tC with different exponents t.

Therefore, now it suffices to show that we can decide whether or not $\varphi(L')$ has two different matrices M and M' such that $M' = MT^t$. Because $\varphi(s^3r) = T$ and $\varphi(r^5s) = T^{-1}$, the following inequivalence implies that there are no such two matrices in S:

$$\varphi(L') \cap \varphi(L' \cdot (\{s^3r\}^+ \cup \{r^5s\}^+)) \neq \emptyset. \tag{4}$$

Note that the unary operator $+$ is called the Kleene plus, and for a set S, the Kleene plus on S, S^+, equals the concatenation of S with the Kleene plus on S, namely $S^+ = SS^*$. Since we know that there is an algorithm that decides whether or not the intersection of two regular subsets of SL$(2,\mathbb{Z})$ is empty [26], the vector ambiguity problem is decidable.

Here we go one step further to show that the vector ambiguity problem is in NP. We use the fact that the inequivalence given in Equation (4) can be brought to the following form of inequivalence:

$$(M_1 + \cdots + M_n)^* C^{-1} \cap (M_1 + \cdots + M_n)^* C^{-1}(T^+ + (T^{-1})^+) \neq \emptyset.$$

This implies that the following regular subset of SL$(2,\mathbb{Z})$ contains the identity matrix:

$$(M_1 + \cdots + M_n)^* C^{-1}(T^+ + (T^{-1})^+) C (M_1^{-1} + \cdots + M_n^{-1})^* = I.$$

Now the vector ambiguity problem reduces to the problem of determining whether the identity matrix is in a regular expression over matrices in SL$(2,\mathbb{Z})$, which is already proven to be in NP [3]. Therefore, we prove that the vector ambiguity problem for matrix semigroups in SL$(2,\mathbb{Z})$ is also in NP. □

Theorem 3.4. The vector ambiguity problem for finitely generated matrix semigroups in SL$(2,\mathbb{Z})$ is NP-complete.

Proof:
The fact that the vector ambiguity problem in SL$(2,\mathbb{Z})$ is in NP is shown in Theorem 3.3. Now we show that it is NP-hard by using an encoding of the *subset sum problem* (SSP) into a set of two-dimensional integral matrices. The SSP is, given a set $U = \{s_1, s_2, \ldots, s_k\}$ of k integers, to decide whether or not there exists a subset $U' \subseteq U$ whose elements sum up to the given integer x. Namely, $\sum_{s \in U'} s = x$.

Define an alphabet $\Sigma = \{0, 1, \ldots, k-1, \ldots, \overline{1}, \overline{2}, \ldots, \overline{k}, a\}$. We define a set W of words which encodes the SSP instance as follows:

$$W = \{i \cdot a^{i+1} \cdot \overline{(i+1)},\ \ i \cdot \varepsilon \cdot \overline{(i+1)},\ \ 0 \cdot a^x \cdot \overline{k} \cdot \sigma \mid 0 \leq i \leq k-1\} \subseteq \{\Sigma \cup \{\sigma\}\}^*.$$

We define 'border letters' as letters from $\Sigma \setminus \{a, \overline{a}\}$ and the inner border letters of a word as all border letters excluding the first and last. We call a word a 'partial cycle' if all inner border letters in that word are inverse to a consecutive inner border letter. Note that any partial cycle $u \in W^+$ is of one of the following forms (i) $i \cdot a^m \cdot \overline{j}$ or (ii) $0 \cdot a^x \cdot \overline{k} \cdot \sigma$, where $i < j$ and m is any integer we can get as a subset sum of integers from s_{i+1} to s_j.

We introduce an additional letter σ which actually encodes the word $c^{2|\Sigma|}$, namely, $\alpha(\sigma) = c^{2|\Sigma|}$ and $f(\alpha(\sigma)) = T^{4|\Sigma|}$. We note that the introduction of the additional letter σ preserves the injectivity of α. For example, any word $w \in \Sigma^*$ of length l has the following image under the mapping α:

$$\alpha(w) = c^{i_1} d' c^{i_2} d' c^{i_3} d' \ldots d' c^{i_{l-1}} d' c^{i_l} d' c^{i_{l+1}},$$

where $-|\Sigma|+1 \leq i_j \leq |\Sigma|$ for $1 \leq j \leq l+1$ and $d' \in \{d, \overline{d}\}$. Now we consider a word $w' \in \{\Sigma \cup \{\sigma\}\}^*$. Then, the image of the word under α is

$$\alpha(w') = c^{i_1} d' c^{i_2} d' c^{i_3} d' \ldots d' c^{i_{l-1}} d' c^{i_l} d' c^{i_{l+1}}.$$

If any i_j for $1 \leq j \leq l+1$ is in a different range, for example, $[(2n-1)|\Sigma|+1, 2n|\Sigma|]$, then we can immediately see that the substring σ^n is used.

Then, we prove that there is a solution to the SSP instance if and only if the matrix semigroup generated by a finite set of matrices corresponding to words in W is ambiguous with respect to a vector $\mathbf{x} = [1, 0]^T$. In other words, there are two matrices M and M' in the matrix semigroup such that

$M\mathbf{x} = M'\mathbf{x}$ and therefore, M' can be represented as MT^t for any non-zero integer t. Assume that there exists a solution to the SSP instance, which is a sequence of integers where the sum of the integers becomes exactly x. Then, the solution can be represented by the following sequence:

$$X = (x_1, x_2, \ldots, x_{k-1}, x_k),$$

where $x_i \in \{0, s_i\}, 1 \leq i \leq k$ and $\sum_{i=1}^{k} x_i = x$.

For a sequence X, there exists a word $w = w_1 w_2 \cdots w_k \in W^+$ such that $w_i = (i-1) \cdot a^{x_i} \cdot \overline{i}$. Since $\sum_{i=1}^{k-1} x_i = x$, the reduced representation of w is $r(w) = 0 \cdot a^x \cdot \overline{k}$ as all inner border letters are cancelled. It follows from that we have two words $0 \cdot a^x \cdot \overline{k}$ and $0 \cdot a^x \cdot \overline{k} \cdot \sigma$ in W^+ if the SSP instance has a solution. Since $f(\alpha(\sigma)) = T^{4|\Sigma|}$, we have two matrices M and M' such that $M' = MT^t$ for a non-zero integer t in the matrix semigroup. Hence, the matrix semigroup is ambiguous with respect to $\mathbf{x}$.

We turn to the opposite direction: if the matrix semigroup is ambiguous with respect to the vector $\mathbf{x}$, then the SSP instance has a solution. Suppose that the matrix semigroup S is ambiguous with respect to $\mathbf{x}$ and there is no solution to the SSP instance. Since S is ambiguous with respect to $\mathbf{x}$, there are two matrices M and M' in S such that $M\mathbf{x} = M'\mathbf{x}$. We also let w and w' be words encoding M and M', respectively. Namely, $f(\alpha(w)) = M$ and $f(\alpha(w')) = M'$.

Since $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} a \\ c \end{pmatrix}$, two matrices M and M' have the same values on their left columns. By Lemma 3.1, M and M' should satisfy the equation $MT^t = M'$ for some non-zero integer $t \in \mathbb{Z}$.

From the fact that $f(\alpha(w)) = M$ and $f(\alpha(w')) = M'$, we have $f(\alpha(w)) \cdot T^t = f(\alpha(w'))$. Since we already have shown in Lemma 2.3 that there are no two words w and w' over Σ satisfying the equation, we can see that either w or w' should end with the special letter σ, which is not in Σ.

Without loss of generality, we assume that w' ends with σ. We also mention that the integer t in the equation should be $4|\Sigma|$ since otherwise we never have a matching word for the part. As we have only one word in W ending with σ, the suffix of w' should be $0 \cdot a^x \cdot \overline{k} \cdot \sigma$. If we summarize the facts, then $w' = w'' \cdot 0 \cdot a^x \cdot \overline{k} \cdot \sigma \in W^+$ for some factorizations $w'' \in W^+$ and w becomes $w'' \cdot 0 \cdot a^x \cdot \overline{k} \in W^+$.

Now we can observe that a word $0 \cdot a^x \cdot \overline{k}$ exists in W^+ if the matrix semigroup is ambiguous with respect to the vector $\mathbf{x}$. As we have mentioned earlier, for any partial cycle $i \cdot a^m \cdot \overline{j}$ in W^+, m is any integer we can get as a subset sum of integers from s_{i+1} to s_j. Therefore, we arrive at a conclusion that the SSP instance has a solution. □

Now we consider the vector non-freeness problem in SL$(2,\mathbb{Z})$.

Theorem 3.5. The vector non-freeness problem for finitely generated matrix semigroups in SL$(2,\mathbb{Z})$ is in NP.

Proof:
Let $S = \langle M_1, M_2, \ldots, M_k \rangle$ be a matrix semigroup and $\mathbf{x}$ be a vector. Let $V = \{\mathbf{v} \mid \mathbf{v} = M\mathbf{x}, M \in S\}$ be a set of target vectors transformed by a matrix in S from $\mathbf{x}$. Then, S is free with respect to $\mathbf{x}$ if there is a unique decomposition of $M \in S$ for every vector $\mathbf{v}$ such that $M\mathbf{x} = \mathbf{v}$.

Therefore, we can check whether or not S is free with respect to $\mathbf{x}$ by checking the existence of two factorizations of matrices that transform $\mathbf{x}$ into a vector in V. In other words, S is not free with respect to $\mathbf{x}$ if we find the following equivalence:

$$M_{s_1} M_{s_2} \ldots M_{s_n} \mathbf{x} = M_{p_1} M_{p_2} \ldots M_{p_m} \mathbf{x},$$

where $s_i, p_j \in [1,k]$ for $1 \leq i \leq n$ and $1 \leq j \leq m$ and $s_i \neq p_i$ for some i. By Equation (2), we can represent these factorizations in the following way:

$$M_{s_1}M_{s_2}\dots M_{s_n} = BT^iC \text{ and } M_{p_1}M_{p_2}\dots M_{p_m} = BT^jC,$$

where $i,j \in \mathbb{Z}$ and $B,C \in \mathrm{SL}(2,\mathbb{Z})$. Since C is in $\mathrm{SL}(2,\mathbb{Z})$, we can multiply the inverse of C to the right and obtain the following equation:

$$M_{s_1}M_{s_2}\dots M_{s_n}C^{-1} = M_{p_1}M_{p_2}\dots M_{p_m}C^{-1}T^{i-j}.$$

Without loss of generality, we assume that $M_{s_1} \neq M_{p_1}$. Now we take the inverse of the right-hand side of the equation.

$$\begin{aligned}(M_{p_1}M_{p_2}\dots M_{p_m}C^{-1}T^{i-j})^{-1}M_{s_1}M_{s_2}\dots M_{s_n}C^{-1} &= I\\ T^{j-i}CM_{p_m}^{-1}\dots M_{p_2}^{-1}M_{p_1}^{-1}M_{s_1}M_{s_2}\dots M_{s_n}C^{-1} &= I\end{aligned} \tag{5}$$

From the above equation, we see that there exists such a multiplication sequence leading to the identity matrix if and only if the matrix semigroup S is not free with respect to the given vector $\mathbf{x}$.

Since the membership problem of a rational subset of matrices in $\mathrm{SL}(2,\mathbb{Z})$ is known to be decidable [13], the vector freeness problem is also decidable, but in exponential space due to translations of matrices in $\mathrm{SL}(2,\mathbb{Z})$ into words over a binary alphabet $\{s,r\}$. Recently, Bell et al. proved that the identity problem for matrix semigroups in $\mathrm{SL}(2,\mathbb{Z})$ is NP-complete [3]. They also showed that the problem of deciding whether the identity matrix is in S, where S is an arbitrary regular subset of $\mathrm{SL}(2,\mathbb{Z})$, is in NP. Since we decide whether a matrix semigroup S in $\mathrm{SL}(2,\mathbb{Z})$ is non-free by checking whether the identity matrix exists in an arbitrary subset of $\mathrm{SL}(2,\mathbb{Z})$ as presented in Equation (5), we prove that the vector non-freeness problem for matrix semigroups in $\mathrm{SL}(2,\mathbb{Z})$ is also in NP. □

In the following, we prove that the vector non-freeness problem is in fact, NP-complete in $\mathrm{SL}(2,\mathbb{Z})$.

Theorem 3.6. The vector non-freeness problem for finitely generated matrix semigroups in $\mathrm{SL}(2,\mathbb{Z})$ is NP-complete.

Proof:
Since we already have shown that the problem is in NP in Theorem 3.5, it only remains to show that the problem is NP-hard. We use an encoding of the *equal subset sum problem* (ESSP) into a set of two-dimensional matrices over integers [30]. The ESSP is, given a set $U = \{s_1, s_2, \dots, s_k\}$ of k integers, to decide whether or not there exist two disjoint nonempty subsets $U_1, U_2 \subseteq U$ whose elements sum up to the same value. Namely,

$$\sum_{s_1 \in U_1} s_1 = \sum_{s_2 \in U_2} s_2.$$

Define an alphabet $\Sigma = \{0,1,\dots,k-1,k,\dots,\overline{1},\overline{2},\dots,\overline{(k-2)},\overline{(k-1)},a\}$. We define a set W of words which encodes the ESSP instance.

$$W = \{i \cdot a^{i+1} \cdot \overline{(i+1)},\ \ i \cdot \varepsilon \cdot \overline{(i+1)} \mid 0 \leq i \leq k-1\} \subseteq \Sigma^*.$$

Note that any partial cycle $u \in W^+$ is of the form $i \cdot a^m \cdot \bar{j}$, where $i < j$ and m is any integer we can get as a subset sum of integers from s_{i+1} to s_j.

We prove the NP-hardness of the vector freeness problem by reducing the equal subset sum problem to the vector freeness problem. As a first step, we show that there is a solution to the given ESSP instance if and only if the matrix semigroup S generated by matrices encoded from the set W is not free with respect to a vector $\mathbf{x} = [1, 0]^T$.

By Lemma 2.3, we can see that S is free with respect to $\mathbf{x}$ if and only if S is free. Therefore, it suffices to show that S is not free if and only if the ESSP instance has a solution.

First we prove that if there is a solution to the ESSP instance, then the matrix semigroup S is not free. Let us assume that there exists a solution to the ESSP instance, which is two sequences of integers where each of two sequences sums up to the same integer x. Then, the solution can be represented by the following pair of sequences:

$$Y = (y_1, y_2, \ldots, y_{k-1}, y_k) \text{ and } Z = (z_1, z_2, \ldots, z_{k-1}, z_k).$$

where $y_i, z_i \in \{0, s_i\}, 1 \leq i \leq k$ and $\sum_{i=1}^{k} y_i = \sum_{i=1}^{k} z_i = x$.

For a sequence Y, there exists a word $w_Y = w_1 w_2 \cdots w_k \in W^+$ such that $w_i = (i-1) \cdot a^{y_i} \cdot \bar{i}$. Since $\sum_{i=1}^{k} y_i = x$, the reduced representation of w_Y is $r(w_Y) = 0 \cdot a^x \cdot \bar{k}$ as all inner border letters are cancelled. Analogously, we have a word w_Z for a sequence Z and its reduced representation $r(w_Z)$ is equal to $r(w_Y)$ as the sum of integers in the sequence Z is equal to the sum of integers in Y. As we have two words in W^+ whose reduced representations are equal, the semigroup generated by matrices encoded from the set W is not free.

Now we prove the opposite direction: if there is no solution to the ESSP instance, then the matrix semigroup S is free. Assume that S is not free. Since the S is not free, we have two different words $w, w' \in W^+$ whose reduced representations are equal, namely, $r(w) = r(w')$.

For a word w, we decompose w into subwords $w = u_1 u_2 \cdots u_m$ such that each $u_i \in W^+, 1 \leq i \leq m$ is a partial cycle of maximal size. Similarly, we decompose w' into subwords of maximal partial cycles as follows: $w' = u'_1 u'_2 \cdots u'_n$. Since $r(w) = r(w')$, it follows that $r(u_i) = r(u'_i)$ should hold for $1 \leq i \leq m$ and $m = n$. On the other hand, since $w \neq w'$, there exists $i, 1 \leq i \leq m$ where $u_i \neq u'_i$. Note that the maximal partial cycles u_i and u'_i should have the same number of a's since $r(u_i) = r(u'_i)$ and the letter a cannot be cancelled by the reduction of words. As we mentioned earlier, the first border letter and last border letter of a partial cycle are integers where the first border letter is strictly smaller than the last border letter. Let us say that i_1 is the first border letter and i_2 is the last border letter of u_i and u'_i. Then, the number of a's in u_i and u'_i is the sum of subset of integers from the set $\{s_{i_1+1}, s_{i_1+2}, \ldots, s_{i_2}\}$. It follows from the fact that $u_i \neq u'_i$ that we have two distinct subsets of the set $\{s_{i_1+1}, s_{i_1+2}, \ldots, s_{i_2}\}$ whose sums are the same. This contradicts our assumption since we have two disjoint subsets of equal subset sum. □

Lastly, we establish the following undecidability as a trivial corollary of Theorem 2 of [1].

Corollary 3.7. The vector freeness problem for finitely generated matrix semigroups over $\mathbb{N}^{3\times 3}$ is undecidable.

Proof:
We first introduce the *mixed modification PCP (MMPCP)* [10] which is already proven to be undecidable

and prove the undecidability of the vector freeness problem over $\mathbb{N}^{3\times 3}$ by encoding an instance of the MMPCP.

Given a finite alphabet Σ, a binary alphabet Δ, and a pair of homomorphisms $h, g : \Sigma^* \to \Delta^*$, the MMPCP asks to decide whether or not there exists a word $w = a_1 \dots a_k \in \Sigma^+, a_i \in \Sigma$ such that

$$h_1(a_1)h_2(a_2)\dots h_k(a_k) = g_1(a_1)g_2(a_2)\dots g_k(a_k),$$

where $h_i, g_i \in \{h, g\}$ and for some $j \in [1, k]$ such that $h_j \neq g_j$.

Note that we use the idea inspired by the undecidability proof for [10].

Let $\Sigma = \{a_1, a_2, \dots, a_{n-2}\}$ and $\Delta = \{a_{n-1}, a_n\}$ be disjoint alphabets and $h, g : \Sigma^* \to \Delta^*$ be an instance of the MMPCP. Define a homomorphism $\alpha : (\Sigma \cup \Delta)^* \to \mathbb{N}$ to be $\alpha(a_{i_1}a_{i_2}\dots a_{i_m}) = \sum_{j=1}^{m} i_j(n+1)^{m-j}$ and $\alpha(\varepsilon) = 0$. Now $\alpha(a_{i_1}a_{i_2}\dots a_{i_m})$ is an $(n+1)$-adic representation of the indices. Then, for any two words w_1 and w_2 over $\Sigma \cup \Delta$, we have the following equation:

$$(n+1)^{|w_2|}\alpha(w_1) + \alpha(w_2) = \alpha(w_1w_2).$$

Define $\gamma : (\Sigma \cup \Delta)^* \times (\Sigma \cup \Delta)^* \to \mathbb{N}^{3\times 3}$ by

$$\gamma(u, v) = \begin{pmatrix} (n+1)^{|u|} & 0 & \alpha(u) \\ 0 & (n+1)^{|v|} & \alpha(v) \\ 0 & 0 & 1 \end{pmatrix}.$$

We can see that γ is a homomorphism since $\gamma(u_1, v_1)\gamma(u_2, v_2) = \gamma(u_1u_2, v_1v_2)$.

Let $G = \{\gamma(a_i, h(a_i)), \gamma(a_i, g(a_i)) \mid a_i \in \Sigma, 1 \leq i \leq n-2\}$ be a generating set of the matrix semigroup S and $\mathbf{x} = [0, 0, 1]^T$ be a vector in $\mathbb{N}^3$. It is not difficult to see that the MMPCP has a solution if and only if there exist two different factorizations over G for a matrix M in S. Since we can uniquely determine any matrix in S by examining the last column of the matrix, we can conclude that the MMPCP has a solution if and only if there exist two different factorizations leading to the same vector. □

4. On the Degree of Vector Ambiguity

Given a matrix semigroup S of $n \times n$ matrices and an n-dimensional vector $\mathbf{x}$, let V be a set of target vectors such that $V = \{\mathbf{y} \mid \mathbf{y} = M\mathbf{x},\ M \in S\}$. Now we consider the problem of determining if there exists a vector $\mathbf{y} \in V$ such that there exists an infinite number of different matrices $M \in S$ such that $M\mathbf{x} = \mathbf{y}$. We call this problem the *finite vector ambiguity problem*.

First remark that if we restrict our attention to the specific target vector $\mathbf{y}$ and consider matrices transforming $\mathbf{x}$ into $\mathbf{y}$, then we can decide whether or not the number of such matrices is infinite.

Theorem 4.1. Given two vectors $\mathbf{x}, \mathbf{y}$ and a finitely generated matrix semigroup S in SL$(2, \mathbb{Z})$, we can decide whether or not $\mathbf{y}$ is finitely ambiguous with respect to S and $\mathbf{x}$.

Proof:
We use a similar approach to the proof of Theorem 3.3. Recall that every matrix M that transforms $\mathbf{x}$ into $\mathbf{y}$ can be represented in the form of BT^tC where $t \in \mathbb{Z}$ and B, C are matrices from SL$(2, \mathbb{Z})$. We

can also compute B and C in polynomial time. Thus, it only remains to count the number of matrices in the form of BT^tC from the matrix semigroup S.

Suppose that we are given n matrices $M_1, M_2, \ldots, M_n$ from $\mathrm{SL}(2,\mathbb{Z})$ as generators of the semigroup S. Namely, $S = \langle M_1, M_2, \ldots, M_n\rangle$. Let $w_1, w_2, \ldots, w_n \in \Sigma^*$ be words encoding the generators, such that $\varphi(w_i) = M_i$ for $1 \le i \le n$. Then, we can define a regular language L corresponding to S over $\Sigma = \{s, r\}$ as $L = \{w_1, w_2, \ldots, w_n\}^+$. Let w_B and w_C be words over $\{s, r\}$ such that $\varphi(w_B) = B^{-1}$ and $\varphi(w_C) = C^{-1}$. Let $L' = \{w_B\} \cdot L \cdot \{w_C\}$. It is easy to see that $\varphi(L') = \{B^{-1}MC^{-1} \mid M \in S\}$.

We also define a regular language L_T corresponding to the set of matrices which are the powers of a matrix T or T^{-1} as follows: $L_T = \{s^3r\}^* \cup \{r^5s\}^*$. In other words, $\varphi(L_T) = \{T^m, T^{-m} \mid m \ge 0\}$. It is important to see that there exists only one word $w \in L_T$ which corresponds to the matrix T^m for any integer m and the word w is always reduced. For instance, ε is the only word in L_T for the matrix $T^0 = \mathbf{I}$ which is the identity matrix.

It remains to construct two signed automata $\mathcal{A}'$ and $\mathcal{A}_T$ for L' and L_T which recognize the set of words in L' and L_T, respectively, also with the set of reduced words corresponding to words in L' and L_T, respectively. Then, we can see that the cardinality of the following set $L' \cap L_T$ implies the number of matrices in S of the form BT^tC with different exponents t.

Since we can decide the finiteness of any regular set of matrices, the problem of deciding whether there exists an infinite number of matrices in S transforming $\mathbf{x}$ into $\mathbf{y}$ is also decidable. □

Theorem 4.2. The finite vector ambiguity problem for finitely generated matrix semigroups in $\mathrm{SL}(2,\mathbb{Z})$ is decidable.

Proof:
Recall that $BT^tC\mathbf{x} = BT^{t'}C\mathbf{x} = \mathbf{y}$ always holds from Lemma 3.2. Therefore, the finite vector ambiguity problem is equivalent to the problem of deciding whether or not there exists a finite number of different matrices M of the form $M = BT^tC$ in the matrix semigroup S such that $M\mathbf{x} = \mathbf{y}$ for every target vector $\mathbf{y}$. Remind that we can compute the matrix C in polynomial time based on the given vector $\mathbf{x} = [x_1, x_2]^T$ such that $C\mathbf{x} = [d, 0]^T$ where $d = \gcd(x_1, x_2)$. In other words, the matrix semigroup S is *finitely ambiguous* with respect to $\mathbf{x}$ if and only if the following condition holds:

$$\max\{x_B \mid B \in \mathrm{SL}(2,\mathbb{Z}),\ \ x_B = |\{t \mid BT^tC \in S\}|\} < \infty, \tag{6}$$

where $C\mathbf{x} = [d, 0]^T$ and $d = \gcd(x_1, x_2)$.

Suppose that we are given n matrices $M_1, M_2, \ldots, M_n$ from $\mathrm{SL}(2,\mathbb{Z})$ as generators of the semigroup S. Let $w_1, w_2, \ldots, w_n \in \Sigma^*$ be words encoding the generators, such that $\varphi(w_i) = M_i$ for $1 \le i \le n$. Then, we can define a regular language L_S corresponding to S over $\Sigma = \{s, r\}$ as $L_S = \{w_1, w_2, \ldots, w_n\}^+$. Then we construct a signed automaton

$$\mathcal{A} = (\langle Q^+, Q^-\rangle, \Sigma, \delta, I, \langle F^+, F^-\rangle)$$

recognizing the language $L_S = \langle L_S^+, L_S^-\rangle$. For every matrix $M \in S$, we have a reduced word $w \in \{s, r\}^*$ in L such that $\varphi(w) = M$ or $\varphi(w) = -M$. Note that if $\varphi(w) = -M$, then $w \in L_S^+$ and otherwise, $w \in L_S^-$.

Consider a subset $Q' \subseteq Q$ of states that satisfies the following condition:

$$\bigcap_{q \in Q'} \{w \mid q \in \delta(I, w)\} \neq \emptyset. \tag{7}$$

This implies that there are paths from the initial state to the states in Q' all labeled by w, which in fact, corresponds to the matrix B.

Now it remains to check whether or not there are words corresponding to an infinite number of matrices of the form T^tC following the word w in the computation of $\mathcal{A}$. The following set $L_{Q'}$ contains words which correspond to matrices D such that $BD \in S$:

$$L_{Q'} = \bigcup_{q \in Q'} \{w \mid f \in \delta(q, w), \quad f \in F\}.$$

Let $w_{C^{-1}} \in \{s, r\}^*$ be a word corresponding to the matrix C^{-1}. Then, the regular language $L_{Q'} \cdot \{w_{C^{-1}}\}$ contains words corresponding to DC^{-1} such that $BD \in S$. Note that it is possible to construct a new signed automaton recognizing all reduced words of $L_{Q'} \cdot \{w_{C^{-1}}\}$ by taking the subset Q' as the set of initial states of $\mathcal{A}$ and extending the final states with the word corresponding to C^{-1}.

Now we see that $L_{Q'} \cdot \{w_{C^{-1}}\}$ contains a matrix of the form T^t if and only if $BT^tC \in S$. Here we make use of the regular language L_T which is defined and used in the proof of Theorem 4.1. Remark that L_T contains a unique reduced word for each power T^m of a matrix T, where m is any integer.

Hence we can decide whether the number of matrices in S of the form BT^tC is finite by deciding whether the following set for each state subset Q' satisfying Equation (7): $(L_{Q'} \cdot \{w_{C^{-1}}\}) \cap L_T$ is finite.

We check the existence of the subset Q' of states satisfying Equation (7) and containing an infinite number of words in $L_{Q'}$ corresponding to T^tC matrices by enumerating all possible state subsets. Therefore, the finite vector ambiguity problem is decidable. □

In the context of semigroup freeness problem, we can also define the *finite vector non-freeness problem* as the problem of determining the existence of a target vector $\mathbf{v} \in V$ which is reachable from the initial vector $\mathbf{x}$ by an infinite number of different factorizations of matrices.

As in the finite vector ambiguity problem, we prove the case when the target vector $\mathbf{y}$ is fixed.

Theorem 4.3. Given two vectors $\mathbf{x}, \mathbf{y}$ and a matrix semigroup S in SL$(2, \mathbb{Z})$, we can decide whether or not $\mathbf{y}$ is finitely non-free with respect to S and $\mathbf{x}$.

Proof:
First we mention that the problem is very similar to the problem of counting the number of matrices that transforms $\mathbf{x}$ into $\mathbf{y}$ considered in Theorem 4.1. The only difference is that we count the number of matrix factorizations instead of matrices from SL$(2, \mathbb{Z})$. Since a matrix $M \in S = \langle M_1, M_2, \ldots, M_n \rangle$ can have multiple factorizations over the generating set $\{M_1, M_2, \ldots, M_n\}$, we cannot count the number of different factorizations of the form BT^tC by constructing singed automata and counting the number of matrices.

Since we are considering the number of factorizations of matrices, we need to keep the unreduced representations of matrices over $\{s, r\}$ instead of considering reduced representations.

Let S be the matrix semigroup generated by the set $\{M_1, M_2, \ldots, M_n\}$. We compute the unique canonical word w_i for each matrix M_i for $1 \leq i \leq n$ and define $L_S = \{w_1, \ldots w_n\}^+$ be the regular language. We also compute two matrices B and C, and let w_B and w_C be the unique canonical words such that $\varphi(w_B) = B$ and $\varphi(w_C) = C$.

Recall that $\varphi(s^3r) = T$ and $\varphi(r^5s) = T^{-1}$. Based on Lemma 2.4, we define a context-free language L_{BT^*C} which is the set of all words corresponding to the set of matrices of the form BT^mC where m is any integer.

Since the intersection between a regular language and a context-free language is a context-free language, the following language L' is also context-free:

$$L' = L_S \cap L_{BT^*C}.$$

For each factorization of matrix M in S, we have a corresponding word in L_S and especially in L' if M can be factorized into BT^mC for some integer m. Note that we may have multiple factorizations of M corresponding to the same word in L_S since two different factorizations of matrices can be to the same matrix. However, it is impossible that infinitely many factorizations of M correspond to a word in L_S since the lengths of some factorizations should be also infinite as we do not consider reduced representation in L_S.

Therefore, we can see that the cardinality of L' is infinite if and only if there exists an infinite number of factorizations $M_1M_2 \dots M_n \in S$ such that $M_1M_2 \dots M_n\mathbf{x} = \mathbf{y}$. Since we can decide whether or not a given context-free language is finite, we show that the problem is decidable. □

We leave open the decidability of the finite vector non-freeness problem. We believe that the problem is also decidable but a little bit more complicated than the finite vector ambiguity problem because there is a possibility of losing some information about factorizations of matrices if we use signed automata in which we consider accepting computations on reduced words over $\{s, r\}$ for corresponding matrices.

Since we have considered the problem of determining finiteness of vector ambiguity of matrix semigroups, it is natural to compute the exact threshold of finitely vector ambiguous matrix semigroups. Given a matrix semigroup S, a vector $\mathbf{x}$, and a non-negative integer k (in unary representation), for every target vector $\mathbf{y}$, does there exist at most k different matrices in S which transform $\mathbf{x}$ into $\mathbf{y}$. We call the problem the *k-vector ambiguity problem*.

Interestingly, the k-vector ambiguity problem is PSPACE-hard by the reduction from the *DFA intersection emptiness problem*. First we start with showing the decidability of the case when we are given both initial and target vectors as follows:

Corollary 4.4. Given two vectors $\mathbf{x}, \mathbf{y}$, a finitely generated matrix semigroup S in $\mathrm{SL}(2, \mathbb{Z})$, and a positive integer $k \in \mathbb{N}$, we can decide whether or not $\mathbf{y}$ is k-ambiguous with respect to S and $\mathbf{x}$.

Proof:
We use a similar approach to the proof of Theorem 4.1. The only difference is that here we need to count the number of matrices of the form BT^tC from the matrix semigroup S instead of deciding the finiteness of the set of such matrices. Since the $L' \cap L_T$ is a regular set and we can simply enumerate every elements of the finite regular set, we can decide whether or not there exist at most k different matrices $M \in S$ such that $M\mathbf{x} = \mathbf{y}$. □

Now we are ready to show that the k-vector ambiguity problem is decidable and PSPACE-hard.

Theorem 4.5. The k-vector ambiguity problem for finitely generated matrix semigroups in $\mathrm{SL}(2, \mathbb{Z})$ is decidable and PSPACE-hard.

Proof:
Recall that $BT^tC\mathbf{x} = BT^{t'}C\mathbf{x} = \mathbf{y}$ always holds from Lemma 3.2. Therefore, the finite vector ambiguity problem is equivalent to the problem of deciding whether or not there exists a finite number of

different matrices M of the form $M = BT^tC$ in the matrix semigroup S such that $M\mathbf{x} = \mathbf{y}$ for every target vector $\mathbf{y}$. Remind that we can compute the matrix C in polynomial time based on the given vector $\mathbf{x} = [x_1, x_2]^T$ such that $C\mathbf{x} = [d, 0]^T$ where $d = \gcd(x_1, x_2)$. In other words, the matrix semigroup S is k-*ambiguous* with respect to $\mathbf{x}$ if and only if the following condition holds:

$$\max\{x_B \mid B \in \mathrm{SL}(2,\mathbb{Z}),\ \ x_B = |\{t \mid BT^tC \in S\}|\} \leq k,$$

where $C\mathbf{x} = [d, 0]^T$ and $d = \gcd(x_1, x_2)$.

Simply speaking, while enumerating all possible state subsets Q' satisfying $\bigcap_{q\in Q'}\{w \mid q \in \delta(I, w)\} \neq \emptyset$, we check the following condition: $|(L_{Q'} \cdot \{w_{C^{-1}}\}) \cap L_T| \leq k$. If there exists a state subset where the above inequality does not hold, we decide that S is not k-ambiguous with respect to $\mathbf{x}$ since there exist more than k matrices in S of the form BT^tC so that the matrices transform $\mathbf{x}$ into the same target vector. Otherwise, S is k-ambiguous with respect to $\mathbf{x}$.

For the PSPACE-hardness of the problem, we reduce the DFA intersection problem [19] to the k-vector ambiguity problem. The DFA intersection problem is, given $k + 1$ DFAs $A_i, 1 \leq i \leq k + 1$, to decide whether or not the intersection of $k + 1$ DFAs is empty.

Let $A_i = (Q_i, \Sigma_A, \delta_i, s_i, F_i)$ be the ith DFA, where $Q_i = \{q_0, q_1, \ldots, q_n\}$ is a finite set of states, Σ_A is an alphabet, δ_i is the transition function, $s_i \in Q_i$ is the start state, and $F_i \subseteq Q_i$ is a finite set of final state. And let us define an alphabet

$$\Sigma = \Sigma_A \cup \{s\} \cup \bigcup_{i=1}^{k+1}(Q_i \cup \overline{Q_i}),$$

where $\overline{Q_i} = \cup_{q\in Q_i}\{\overline{q}\}$. We also define a set W of words which encodes the instance of the DFA intersection problem as follows. For each transition $p \in \delta_i(q, a)$ of A_i, we add a word $q \cdot a \cdot \overline{p}$ to the set W. For each start state s_i of A_i, we add $s \cdot s_i$. Then, it is very easy to see that $s \cdot w \cdot \overline{f_i} \in W^+$, where $f_i \in F_i$, if and only if $w \in L(A_i)$. Let us define an additional letter σ which encodes the word $c^{2|\Sigma|}$, namely, $\alpha(\sigma) = c^{2|\Sigma|}$ and $f(\alpha(\sigma)) = T^{4|\Sigma|}$. Now we additionally add the following words to the set W. For each final state f_i of A_i, $\{f_i \cdot \sigma^i \mid f_i \in F_i\} \subseteq W$. Then, we have $s \cdot w \cdot \sigma^i \in W^+$ if and only if $w \in L(A_i)$.

We claim that S_W is k-free with respect to the vector $[1, 0]^T$ if and only if the intersection of $k + 1$ DFAs is empty. We first prove that if S_W is k-free with respect to the vector $[1, 0]^T$, then the intersection of DFAs is empty. Assume that the intersection of $k + 1$ DFAs is not empty to prove by contradiction. This implies that there is a word that can be accepted by DFAs $A_1, \ldots A_{k+1}$. Therefore, there are $k + 1$ words in W^+ as follows: $s \cdot w \cdot \sigma^i \in W^+$ for $1 \leq i \leq k + 1$.

Since $f(\alpha(\sigma)) = T^{4|\Sigma|}$ and we have $k + 1$ matrices in S_W which can be represented as follows: $BT^{4|\Sigma|i} \in S_W$ for $1 \leq i \leq k + 1$, where B is a matrix from $\mathrm{SL}(2,\mathbb{Z})$. By Lemma 3.2, we have a contradiction since S_W is not k-free with respect to $[1, 0]^T$.

Now we prove the opposite direction. Assume that S_W is not k-free with respect to $[1, 0]^T$. This implies that there are at least $k+1$ matrices $M_1, \ldots, M_{k+1} \in S_W$ where each matrix can be decomposed into the form of BT^t. Since $M_i \in S_W, 1 \leq i \leq k + 1$, we have a corresponding word $w_i \in W^+, 1 \leq i \leq k + 1$ such that $f(\alpha(w_i)) = M_i$. By Lemma 2.3, each word w_i should be ending with a distinct number of special symbols σ. Moreover, since $k + 1$ DFAs are not connected to each other, w_i should start with s which is an imaginary state connected to every state state of $k + 1$ DFAs by ε-transitions.

Since the symbol σ only appears after canceling a final state, the word w_i should be of the form $s \cdot w \cdot \sigma^i$, where $w \in L(A_i)$.

We reach the contradiction since there exists a word w that can be spelled out by all $k+1$ DFAs and thus, the intersection of DFAs is not empty. Note that the reduction process can be done in polynomial time. Hence, we prove that the k-vector ambiguity problem in SL$(2, \mathbb{Z})$ is PSPACE-hard. □

Remark that the k-vector ambiguity problem is in fact, in EXPSPACE as the size of signed automata can be exponentially large in the size of representation of matrix semigroup S. Therefore, we have an EXPSPACE upper bound and PSPACE-hard lower bound for the k-vector ambiguity problem. However, the PSPACE-hardness still applies even if we are given all numeric values of the input in unary representation. Moreover, the size of signed automata stays polynomial if we assume that the input is given in unary representation. Hence, we have the following interesting corollary:

Corollary 4.6. The k-vector ambiguity problem for finitely generated matrix semigroups in SL$(2, \mathbb{Z})$ is PSPACE-complete if we are given all numeric values of the input in unary representation.

Lastly, we consider the k-vector non-freeness problem in which we consider the finite number of different factorizations transforming the given vector $\mathbf{x}$ into any target vector. As in the k-vector ambiguity case, the k-vector freeness problem is decidable if we are given a target vector $\mathbf{y}$ as follows:

Theorem 4.7. Given two vectors $\mathbf{x}, \mathbf{y}$, a finitely generated matrix semigroup S in SL$(2, \mathbb{Z})$, and a positive integer $k \in \mathbb{N}$, we can decide whether or not $\mathbf{y}$ is k-non-free with respect to S and $\mathbf{x}$.

Proof:
Note that the proof is based on the proof of Theorem 4.3. Recall that the context-free language L' contains (unreduced) words which are concatenations of canonical words corresponding to generators of the matrix semigroup S. Moreover, for every word w in L', the matrix $\varphi(w)$ can be decomposed as BT^mC for some integer m. It is easy to see that if S has at most k different factorizations of matrices transforming $\mathbf{x}$ into $\mathbf{y}$, then $|L'|$ is finite. The only concern is that some word in L' may correspond to multiple factorizations of matrices. We can resolve this problem by counting the number of accepting runs for each word in L' from an NFA $\mathcal{A}_S$ accepting L_S. Let $\beta(w)$ be the number of accepting runs of $w \in L'$ on $\mathcal{A}_S$. Then, we can conclude that there are $\sum_{w \in L'} \beta(w)$ different factorizations of matrices transforming $\mathbf{x}$ into $\mathbf{y}$. □

Acknowledgements

This research was supported by EPSRC grant EP/M00077X/1.

References

[1] Bell, P. C., Chen, S., Jackson, L.: Scalar Ambiguity and Freeness in Matrix Semigroups over Bounded Languages, *Proceedings of the 10th International Conference on Language and Automata Theory and Applications*, 2016.

[2] Bell, P. C., Hirvensalo, M., Potapov, I.: Mortality for 2×2 Matrices Is NP-Hard, *Proceedings of the 37th International Symposium on Mathematical Foundations of Computer Science*, 2012.

[3] Bell, P. C., Hirvensalo, M., Potapov, I.: The Identity Problem for Matrix Semigroups in $\mathrm{SL}_2(\mathbb{Z})$ is NP-complete, *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*, 2017.

[4] Bell, P. C., Potapov, I.: Periodic and Infinite Traces in Matrix Semigroups, *Proceedings of the 34th Conference on Current Trends in Theory and Practice of Computer Science*, 2008.

[5] Bell, P. C., Potapov, I.: Reachability problems in quaternion matrix and rotation semigroups, *Information and Computation*, **206**(11), 2008, 1353–1361.

[6] Bell, P. C., Potapov, I.: On the Computational Complexity of Matrix Semigroup Problems, *Fundamenta Infomaticae*, **116**(1-4), 2012, 1–13.

[7] Birget, J.-C., Margolis, S. W.: Two-letter group codes that preserve aperiodicity of inverse finite automata, *Semigroup Forum*, **76**(1), 2008, 159–168.

[8] Blondel, V. D., Cassaigne, J., Karhumäki, J.: Problem 10.3: Freeness of multiplicative matrix semigroups, in: *Unsolved Problems in Mathematical Systems and Control Theory*, Princeton University Press, 2004, 309–314.

[9] Cassaigne, J., Harju, T., Karhumäki, J.: ON THE UNDECIDABILITY OF FREENESS OF MATRIX SEMIGROUPS, *International Journal of Algebra and Computation*, **9**(3-4), 1999, 295–305.

[10] Cassaigne, J., Karhumäki, J., Harju, T.: *On the Decidability of the Freeness of Matrix Semigroups*, Technical report, Turku Center for Computer Science, 1996.

[11] Chamizo, F.: Non-Euclidean visibility problems, *Proceedings of the Indian Academy of Sciences - Mathematical Sciences*, **116**(2), 2006, 147–160.

[12] Charlier, E., Honkala, J.: The freeness problem over matrix semigroups and bounded languages, *Information and Computation*, **237**, 2014, 243–256.

[13] Choffrut, C., Karhumäki, J.: Some decision problems on integer matrices, *RAIRO - Theoretical Informatics and Applications*, **39**(1), 3 2010, 125–131.

[14] Elstrodt, J., Grunewald, F., Mennicke, J.: Arithmetic Applications of the Hyperbolic Lattice Point Theorem, *Proceedings of the London Mathematical Society*, **s3-57**(2), 1988, 239–283.

[15] García del Moral, M. P., Martín, I., Peña, J. M., Restuccia, A.: $\mathrm{SL}(2, \mathbb{Z})$ symmetries, supermembranes and symplectic torus bundles, *Journal of High Energy Physics*, **2011**(9), 2011, 68.

[16] Gurevich, Y., Schupp, P.: Membership Problem for the Modular Group, *SIAM Journal on Computing*, **37**(2), 2007, 425–459.

[17] Klarner, D. A., Birget, J.-C., Satterfield, W.: ON THE UNDECIDABILITY OF THE FREENESS OF INTEGER MATRIX SEMIGROUPS, *International Journal of Algebra and Computation*, **01**(02), 1991, 223–226.

[18] Ko, S.-K., Potapov, I.: Matrix Semigroup Freeness Problems in $\mathrm{SL}(2, \mathbb{Z})$, *Proceedings of the 43rd Conference on Current Trends in Theory and Practice of Computer Science*, 2017.

[19] Kozen, D.: Lower Bounds for Natural Proof Systems, *Proceedings of the 18th Annual Symposium on Foundations of Computer Science*, 1977.

[20] Lyndon, R. C., Schupp, P. E.: *Combinatorial group theory*, Springer Berlin Heidelberg, 1977.

[21] Mackenzie, D.: A new twist in knot theory, in: *What's Happening in the Mathematical Sciences*, vol. 7, American Mathematical Society, 2009, 3–17.

[22] Mandel, A., Simon, I.: On finite semigroups of matrices, *Theoretical Computer Science*, **5**(2), 1977, 101–111.

[23] Noll, T.: Musical intervals and special linear transformations, *Journal of Mathematics and Music*, **1**(2), 2007, 121–137.

[24] Polterovich, L., Rudnick, Z.: Stable mixing for cat maps and quasi-morphisms of the modular group, *Ergodic Theory and Dynamical Systems*, **24**, 2004, 609–619.

[25] Potapov, I.: Composition Problems for Braids, *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science*, 24, 2013.

[26] Potapov, I., Semukhin, P.: Vector Reachability Problem in SL$(2, \mathbb{Z})$, *Proceedings of the 41st International Symposium on Mathematical Foundations of Computer Science*, 2016.

[27] Potapov, I., Semukhin, P.: Decidability of the Membership Problem for 2×2 integer matrices, *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*, 2017.

[28] Shallit, J.: *A Second Course in Formal Languages and Automata Theory*, 1 edition, Cambridge University Press, New York, NY, USA, 2008.

[29] Witten, E.: SL$(2, \mathbb{Z})$ action on three-dimensional conformal field theories with abelian symmetry, in: *From fields to strings: circumnavigating theoretical physics*, vol. 2, World Scientific Publishing, 2005, 1173–1200.

[30] Woeginger, G. J., Yu, Z.: On the equal-subset-sum problem, *Information Processing Letters*, **42**(6), 1992, 299–302.

[31] Zagier, D.: Elliptic Modular Forms and Their Applications, in: *The 1-2-3 of Modular Forms: Lectures at a Summer School in Nordfjordeid, Norway*, Springer Berlin Heidelberg, 2008, 1–103.